Best Practices Guide

McAfee VirusScan Enterprise for Linux 2.0

Best practices for ideal protection

Best practices are the proven approach that provides optimum protection to your systems.

If your requirement varies for your environment, use the best practices recommendation as a baseline. When applied, this protection approach helps you to:

- Protect your system from malware threats in real time.
- Keep the scanning engine and DAT files up to date which is critical to detect latest malware threats.
- Make sure that your system does not contain infected files.

Introduction

McAfee® VirusScan® Enterprise for Linux protects your Linux systems from malware threats and potentially unwanted software.

The software protects your Linux systems from malware threats, such as, viruses, trojan horses, spyware, keyloggers, joke programs, and potentially unwanted software.

System requirements

Make sure that your system meets these minimum requirements, and you have administrator rights.

Component	Requirements
Processors	• Intel x86_64 architecture-based processor that supports Intel Extended Memory 64 technology. (Intel EM64T) • AMD x86_64 architecture-based processor with AMD 64-bit technology
Memory	Minimum: 2 GB RAM Recommended: 4 GB RAM
Free Disk space	Minimum: 1 GB

Component	Requirements

Operating Systems (64-bit)	• Operating system 64-bit
	  • SUSE Linux Enterprise Server 11 SP2 64-bit
	  • SUSE Linux Enterprise Server 11 SP3 64-bit
	  • Ubuntu 12.04, 12.10, 13.04, and 13.10 64-bit
	  • Amazon Linux AMI 2013.03 64-bit
	  • SUSE and Ubuntu on Amazon Elastic Compute Cloud (Amazon EC2)
	  • Novell Open Enterprise Server 11 SP1
	  This product cannot be used on 32-bit platforms.
	• Virtual platforms
	  • VMware
	  • Citrix Xen
	  • Xen
	  • KVM
	  • Virtual box
	  • Paravirtual environment
	  • Guest operating system on Xen Hypervisor

McAfee Management software	• McAfee ePolicy Orchestrator 4.6 • McAfee ePolicy Orchestrator 5.0 • McAfee ePolicy Orchestrator 5.1
McAfee Agent	McAfee Agent 4.8 Patch 2

Pre-installation

Before installing the software on a standalone system or managed systems, McAfee recommends that you check these items.

Standalone system

Before installing the software, make sure that:

- The `/opt` and `/var` directories have the minimum required space available.
- The processor and memory requirements are met.
- You have root or sudo permissions.
- There are no third-party anti-virus products installed on your system.
- See the product release notes for the list of known issues.

Managed system

Before deploying the software:

- Make sure that McAfee Agent and its extensions are checked in to the ePolicy Orchestrator repository.
- You can directly deploy McAfee Agent from ePolicy Orchestrator 4.6.x or later by clicking the **New Systems** tab and pushing the non-Windows agent to the Linux client system.
- To deploy the software with customized settings, copy the nails.options file to the `/root` and `/directory` on your Linux client system.
- Copy the `install.sh` file from ePolicy Orchestrator to your Linux clients using SCP, FTP, or by downloading the `install.sh` file from a browser to your managed system. Make sure that the file is transferred in binary mode while using FTP to avoid file corruption.
- Make sure that there are no third-party anti-virus products installed on your managed systems.

When upgrading from the evaluation version to the licensed version, upgrade the software before the evaluation period expires.

Novell Open Enterprise Server

Before installing the software on Novell Open Enterprise Server (standalone and managed systems):

- Create a user (nails) and group (nailsgroup) in your eDirectory.
- Verify the operating system is able to resolve the user name and user group from eDirectory. Install the software only after the user name and user group is created successfully. For more information for resolving the user name and user group, see the user manual of the your operating system version.
- Enable LUM (Linux User Management) for the user and group.
- Provide user with supervisor rights on all NSS volumes. Make sure that the user has supervisor rights on all NSS volumes that are added.

Post-installation

After installing the software on a standalone system or managed systems, McAfee recommends that you perform these tasks.

- Confirm that the software uses the latest engine and DAT files.
- Verify the on-access scanning and on-demand scanning features using the EICAR test malware file. For more information, see *McAfee VirusScan Enterprise for Linux 2.0 Product Guide*.
- Schedule the DAT and Engine update. Using the latest DAT files, the software can detect and take action on the latest malware threats. McAfee recommends that you update DAT files daily and regularly check the McAfee Labs website for the latest updates.
- Run an immediate on-demand scan for all directories and network-mounted volumes to make sure that your system does not contain infected files.
- Verify the managed systems' details in the **System Tree** page of ePolicy Orchestrator.

Engine and DAT update

You must keep your software up to date to make sure your system is protected from the latest threats.

McAfee releases updated DAT files daily to identify and take action against recent threats. Using the latest DAT files is important to detect the latest threats.

Make sure that at least 500 MB of memory is free before a DAT update.

On-access scan settings

On-access scanning is the prime defense point to protect your systems.

Always select on-access scanning to scan all files when reading from and writing to disk.

Here are the best practices for configuring on-access settings on a standalone system or managed systems. The settings can vary according to your requirements.

- Make sure that the software scans all types of files that are accessed.
- Disable the **Scan files on network-mounted volumes (NFS, CIFS/SMBFS only)** option to increase performance. Enable this option only if you can't install McAfee anti-malware solution on your network servers.
- Enable the **Quarantine** option always as a secondary action for virus detections. Enabling this option allows you to retrieve the files from the quarantine folder later, if needed.
- In **On-access settings**, set the **Action if scan error occurs** option to **Deny access**.
- Disable **Decompress archives** to increase performance. Scanning archive files in on-access scanning might significantly impact system performance. McAfee recommends that you schedule an on-demand scan during non-business hours. Although malware is stored in the archive file, the software finds malware when these archive files are read or decompressed.

On-demand scanning

Scheduling on-demand scanning at regular intervals makes sure that your system does not contain infected files.

- Schedule the on-demand scan during non-business hours such as weekends, during the maintenance period, or when DAT and engine updates are not running.
- When scheduling an on-demand scan for the first time, schedule a full on-demand scan for the local volumes.
- Make sure to exclude network-mounted volumes, if you do not want to scan them explicitly.
- Always enable the **Decompress archives** option to scan inside the archives and compressed files.
- Enable the **Quarantine** option as a secondary action for virus detections. Enabling this option allows you to retrieve the files from the quarantine folder later, if needed.

Excluding files and directories

Configure the exclusion option to avoid scanning the files used by the system.

McAfee suggests these exclusions for better performance. You can tweak these exclusions based on your requirements.

The software supports regular expression-based exclusions for anti-malware. You can add regular expressions that match the required pattern to exclude multiple files and folders from being scanned.

Some of the recommended exclusions are:

- Oracle database files
  - /opt/oracle/.*\.dbf (if oracle is installed under /opt)
  - /opt/oracle/.*\.ctl (if oracle is installed under /opt)
  - /opt/oracle/.*\.log (if oracle is installed under /opt)
- Evolution data files
- Thunderbird data files
- Encrypted files
- /var/log for on-access scanning
- /quarantine and /proc for on-demand scanning
- JAR files for on-access scanning

  If you exclude the JAR file from on-access scanning, always run an on-demand scan on the JAR file before accessing the file.
- Archive files for on-access scanning
- DTX files for on-access scanning
- WAR files
- exclude groupwise folders
- On an Open Enterprise Server, exclude:
  - `/media/nss/<VOLUME_NAME>/._NETWARE`
  - `/media/nss/<VOLUME_NAME>/._ADMIN`

The following are examples of regular expressions that you can use for different patterns.

Table 1 Regular expression examples

To exclude...	Use...
All files starting with **abc** available in /media/nss	`/media/nss/abc.*`
All files starting with "**.**" under /media/nss	`/media/nss/\..*`
All files with extensions ext and abc under /media/nss	`/media/nss/.*\.(ext|abc)`
All users mailbox folders	`/home/.*/mailbox/.*`
All files and folders starting with abc in the system	`.*/abc.*`
Files with extension .mdb	`.*\.mdb`
Files with extension .mdb or .odc	`.*\.(mdb|odc)`
Files with extension .jar or .rar or .war under /opt	`/opt/.*..+ar`
All files under /tmp starting with a letter and ending with a number	`/tmp/([A-Z]|[a-z]).*[0-9]$`
All files ending with abc, abcc, abcccc	`.*abc{1,}`

McAfee recommends that you configure the **On-Access Settings** and **On-Demand Settings** page to scan all files.

Using regular expressions from ePolicy Orchestrator

- You must include `/` as the first character. For example, to exclude all files and folders starting with abc in the system, use the regular expression: `/.*/abc.*`

Default configuration

These are the default scanning options that are changed from the previous version of the software.

On-access settings

These on-access scanning options are unselected by default. However, you can configure the settings according to your environment.

- **Decompress archives** — Unselected.
- **Scan files on network-mounted volumes (NFS,CIFS/SMBFS only)** — Unselected.

The default exclusions for on-access scanning:

- /_admin/Manage_NSS
- /media/nss/.*/(\._NETWARE|\._ADMIN)
- * /.*\.(vmdk|VMDK|dbl|DBL|ctl|CTL|log|LOG|jar|JAR|war|WAR|dtx|DTX|dbf|DBF|frm|FRM|myd|MYD|myi|MYI|rdo|RDO|arc|ARC)

On-demand settings

The default exclusions for on-demand scanning:

- / quarantine

McAfee recommends you verify the default scanning settings and configure the settings according to your environment.

Default queries for managed systems

A graphical report for compliance and threat summary.

McAfee ePO has its own querying and reporting capabilities. When the software reports that the extension is installed, it provides a set of default queries. However, you can create a new query, edit, and manage all the queries related to the software.

By default there are two queries you can generate to know the managed system status.

Table 2 VirusScan Enterprise for Linux — Default queries

Query	Description
VSEL: VirusScan Enterprise for Linux Compliance	Shows a graphical display of the compliant and non-compliant linux systems in the network. When you run this query, you can see the system showing up in the report.
VSEL: VirusScan Enterprise for Linux Threats	Shows a graphical display of the threat summary and action taken on all Linux systems in the network.

Third-party software coexistence

Make sure that there is no third-party software exists in the system.

- The software does not support coexistence with backup software such as *ArcServe*, *Cava Agent*, *bacula* backup software. McAfee recommends that you exclude directories or files associated with it.
- The software supports *bmcpatrol* and McAfee Application Control.

Tips and tricks

These tips and tricks can be helpful when using and configuring the software.

- You can deploy the software from ePolicy Orchestrator with customized settings. For this you must copy the nails.options file to the /root and / directory on your managed systems.
- McAfee recommends you to enable advanced logging option for troubleshooting. These settings **Detail logging level**, **Additional log to syslog**, **Detail syslog level**, **Limit age of log entries**, **Maximum age of log entries** can be enabled from the managed system or from ePolicy Orchestrator.
- In a managed mode, the status of scheduled tasks is not reported back to ePolicy Orchestrator. Instead, set up **SMTP email notifications** can monitor this. Users receives email notification if the DAT is out of date, if malware is detected on the system, and notification based on error codes including system events on the user's email id.
- Remove the local tasks from the managed system, if they are not required.
- View the default configuration setting on each page, and configure the settings as required for your environment.
- By default, the software uses the system PAM (Pluggable Authentication Modules) configuration in the **Web Manager** for authentication. In some instances, the system PAM settings might use external authentication modules that are not compatible with the software. For information about configuring PAM, so that the software can authenticate in the web manager, see McAfee KnowledgeBase article KB70568.

Contact information

Use this contact information such as the threat center, download site, technical support, customer service, and professional services.

McAfee Threat Center

McAfee Labs: http://www.mcafee.com/us/mcafee_labs/index.html

McAfee Threat Center: http://vil.mcafeesecurity.com

McAfee Labs .DAT Notification Service Opt-In: https://secure.mcafee.com/apps/mcafee-labs/dat-notification-signup.aspx

McAfee Technical Support

Homepage: http://www.mcafee.com/us/support/index.html

KnowledgeBase Search: http://knowledge.mcafee.com

McAfee Technical Support portal (For logon credentials): https://mysupport.mcafee.com/eservice_enu/start.swe

McAfee customer service

Web: http://www.mcafee.com/us/support/index.html or http://www.mcafee.com/us/about/contact/index.html

Phone: +1-888-VIRUS NO or +1-888-847-8766 Monday - Friday, 8 a.m. — 8 p.m., Central Time

McAfee professional services

Enterprise: http://www.mcafee.com/us/enterprise/services/index.html

Small and Medium Business: http://www.mcafee.com/us/smb/services/index.html

Copyright © 2014 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

McAfee
An Intel Company